# A FAMILY OF MARKOV SHIFTS (ALMOST) CLASSIFIED BY PERIODIC POINTS

Thomas Ward

2 December 1997

*Journal of Number Theory, to appear.*

Abstract. Let $G$ be a finite group, and let

$$X_G = \{\mathbf{x} = (x_{(s,t)}) \in G^{\mathbb{Z}^2} \mid x_{(s,t)} = x_{(s,t-1)} \cdot x_{(s+1,t-1)} \text{ for all } (s,t) \in \mathbb{Z}^2\}.$$

The compact zero–dimensional set $X_G$ carries a natural shift $\mathbb{Z}^2$–action $\sigma^G$ and the pair $\Sigma_G = \left(X_G, \sigma^G\right)$ is a two–dimensional topological Markov shift.

Using recent work by Crandall, Dilcher and Pomerance on the Fermat quotient, we show the following: if $G$ is abelian, and the order of $G$ is not divisible by 1024, nor by the square of any Wieferich prime larger than $4 \times 10^{12}$, and $H$ is any abelian group for which $\Sigma_G$ has the same periodic point data as $\Sigma_H$, then $G$ is isomorphic to $H$.

This result may be viewed as an example of the "rigidity" properties of higher–dimensional Markov shifts with zero entropy.

## 1. Introduction

Let $G$ be a finite group, and define

$$X_G = \{\mathbf{x} = (x_{(s,t)}) \in G^{\mathbb{Z}^2} \mid x_{(s,t)} = x_{(s,t-1)} \cdot x_{(s+1,t-1)} \text{ for all } (s,t) \in \mathbb{Z}^2\}. \tag{1}$$

The set $X_G$ is a closed subset of $G^{\mathbb{Z}^2}$, and inherets from the discrete topology on $G$ a topology in which it is compact and totally disconnected. The natural shift $\mathbb{Z}^2$–action defined by

$$\sigma^G_{(n,m)}(\mathbf{x})_{(s,t)} = x_{(n+s,m+t)} \tag{2}$$

makes the pair $\Sigma_G = \left(X_G, \sigma^G\right)$ into a two–dimensional topological Markov shift.

If the alphabet group $G$ is abelian, then $X_G$ is again a group, and the action $\sigma^G$ is by automorphisms. This example (with $|G| = 2$) was introduced by Ledrappier in [2], and various generalizations have been studied both as a topological dynamical

---

1991 *Mathematics Subject Classification.* 58F20, 54H20.

The author gratefully acknowledges support from NSF grant DMS-94-01093 at the Ohio State University

system and as a measurable dynamical system (see [8], [9], [10], [11]). A general discussion of higher–dimensional subshifts of finite type may be found in [6].

Two $\mathbb{Z}^2$–actions $\sigma_1$ on $X_1$ and $\sigma_2$ on $X_2$ are topologically conjugate if there is a homeomorphism from $X_1$ to $X_2$ that intertwines the actions $\sigma_1$ and $\sigma_2$. Shereshevsky [8] has shown that a topological conjugacy between $\sigma_G$ and $\sigma_H$ must itself preserve the algebraic structure, and so requires $G$ and $H$ to be isomorphic. Our purpose is to try and prove this result by simple counting arguments, and starting with the *a priori* weaker and more dynamical hypothesis of equal numbers of periodic points for each period. The partial results obtained is an instance of the extreme "rigidity" properties of higher–dimensional algebraic dynamical systems with zero entropy (cf. Theorem 31.1 in [7]).

A period for a $\mathbb{Z}^2$–action $\sigma$ by homeomorphisms of a set $X$ is a subgroup $\Gamma \subset \mathbb{Z}^2$ with finite index, and the set of $\Gamma$–periodic points is

$$Fix_\Gamma(\sigma) = \{x \in X \mid \sigma_{\mathbf{n}}(x) = x \text{ for all } \mathbf{n} \in \Gamma\}.$$

It is clear that the cardinality $F_\Gamma(\sigma) = |Fix_\Gamma(\sigma)|$ is an invariant of topological conjugacy.

**Conjecture.** *If $G$ and $H$ are finite abelian groups, and $F_\Gamma(\sigma^G) = F_\Gamma(\sigma^H)$ for all periods $\Gamma$, then $G$ and $H$ are isomorphic.*

At the opposite extreme, if $G$ is any finite group then the shift action on the positive entropy Markov shift $G^{\mathbb{Z}^2}$ has exactly $|G|^m$ points of period $\Gamma$ for any $\Gamma$ with index $m$ in $\mathbb{Z}^2$, so knowing the number of periodic points reveals nothing about the group $G$.

What can be shown quickly is a version of this conjecture that places restrictions on the orders of $G$ and $H$; with a little more effort less restrictive conditions need be imposed, and the conjecture is based on the view that with further calculations, more obstructions can be removed. A proof of the conjecture in full generality seems to require different methods.

My thanks to Prof. Ron Solomon for discussions related to finite groups, Prof. Dan Hendrick for help with calculations, Prof. Les Reid for help with Lemma 2 and Prof. David Sibley for showing me the argument in Lemma 6. I also thank an anonymous referee for finding a serious mistake in one of the calculations and for suggestions leading to strengthened results.

## 2. Abelian alphabets

The number of points of given period in $\Sigma_G$ is given by the number of solutions of certain equations with variables in $G$. These numbers carry some information about $G$, so the strategy is to use these numbers to reconstruct $G$.

**Example.** If $G$ is an abelian group with $|G| = 8$, then the structure of $G$ is determined by the number of solutions to the equation $2x = 0$. If $G$ is any group

with $|G| = 8$, then the structure of $G$ is determined by the number of solutions to the pair of equations $2x = 0$, $4y = 0$.

For any finite group $G$, let $G(n) = |\{g \in G \mid ng = e\}|$.

**Definition 1.** A sequence of natural numbers $\{a_n\}$ is called *$p$–good* for a rational prime $p$ if, for every $k \geq 1$, there is an $n$ for which $p^k | a_n$ and $p^{k+1} \not| a_n$.

**Lemma 2.** *Let $p$ be a fixed prime, and let $G$ be a finite abelian group. Then the quantities $G(p)$, $G(p^2), \ldots, G(p^n)$ determine the structure of the $p$–primary component of $G$ if and only if $|G|$ is not divisible by $p^{2n+2}$.*

*Proof.* See Appendix. □

**Lemma 3.** *If $G$ is a finite abelian group, and $\{a_n\}$ is $p$–good, then the structure of the $p$–primary component of $G$ is determined by the sequence of numbers $\{G(a_n)\}$.*

*Proof.* This follows at once from Definition 1 and Lemma 2. □

Recall that an odd prime $p$ is a *Wieferich prime* if

$$2^{p-1} \equiv 1 \pmod{p^2}. \tag{3}$$

See [12] for the first appearance of these numbers and their connection to Fermat's theorem, and [1], [5] for modern perspectives on the prevalence of these numbers and their history.

**Lemma 4.** *If $p$ is an odd prime that is not a Wieferich prime, then $\{2^n - 1\}$ is $p$–good.*

*Proof.* First notice that $2^{p-1} \equiv 1 \bmod p$, so that the case $k = 1$ is immediate. We now claim that if $p^n | 2^k - 1$ and $p^{n+1} \not| 2^k - 1$ then $p^{n+1} | 2^{pk} - 1$ and $p^{n+2} \not| 2^{pk} - 1$. This follows from more general results – see for instance Theorem 7 and the Introduction of [3]. A direct proof follows from the binomial theorem: let $w, x, y, z$ denote integers, and let $r$ be the multiplicative order of 2 modulo $p$. Then

$$2^r = 1 + xp + yp^2,$$

and $p$ is Wieferich if $p|x$. On the other hand, $r|(p-1)$ by Fermat's little theorem, so

$$2^{(p-1)} = (2^r)^{(p-1)/r} = 1 + x\left(\frac{p-1}{r}\right)p + zp^2.$$

It follows that if $p$ does not divide $x$ then

$$2^{rp^k} = 1 + xp^{k+1} + wp^{k+2},$$

which shows that $\{2^n - 1\}$ is $p$–good. □

The partial result that suggests the conjecture of Section 1 now follows by a calculation.

**Theorem 5.** *Let $G$ and $H$ be finite abelian groups. If $|G|$ is not divisible by 1024 nor by the square of any Wieferich prime larger than $4 \times 10^{12}$, and $F_\Gamma(\sigma^G) = F_\Gamma(\sigma^H)$ for all periods $\Gamma$, then $G$ and $H$ are isomorphic.*

*Proof.* The proof proceeds by using data from specific periods to determine the structure of the $p$–primary component of $G$ for various primes $p$.

(1) Primes larger than $4 \times 10^{12}$.

Let $\Gamma_1(k) = \mathbb{Z} \times (0,k)\mathbb{Z} \subset \mathbb{Z}^2$. A point $\mathbf{x} \in X_G$ with period $\Gamma_1(k)$ is then a member of $G^{\mathbb{Z}^2}$ with the properties $x_{(s,t)} = x_{(s,t-1)} + x_{(s+1,t-1)}$, $x_{(s+1,t)} = x_{(s,t)}$ and $x_{(s,t+k)} = x_{(s,t)}$. Solving these simultaneous equations in $G$ gives:

$$2^k x_{(0,0)} = x_{(0,0)},$$

and all the other coordinates $x_{(s,t)}$ are determined once $x_{(0,0)}$ is, so

$$F_{\Gamma_1(k)}(\sigma^G) = G(2^k - 1).$$

It follows that the structure of the $p$–primary component of $G$ is determined for $p > 4 \times 10^{12}$: if $p$ is Wieferich then it only appears once and is a factor of $2^k - 1$ for some $k$, if $p$ is not Wieferich then by Lemma 3 and Lemma 4 the sequence $\{G(2^k - 1)\}$ determines the structure.

(2) Odd primes smaller than $4 \times 10^{12}$ other than 1093 and 3511.

By work of Crandall, Dilcher and Pomerance on the Fermat quotient (see [1]), none of these primes are Wieferich primes. Using the same periods as in (1), the quantities $\{G(2^k - 1)\}$ are determined by the periodic point data, so the structure of the $p$–primary component of $G$ is determined for all primes under consideration.

(3) The prime 3511.

This is the larger of the two known Wieferich primes. It follows that the periods used in (1) and (2) above cannot distinguish between the cyclic group of order $3511^2$ and the elementary abelian group of order $3511^2$.

Let $\Gamma_2(k)$ be the finite index subgroup of $\mathbb{Z}^2$ defined by

$$\Gamma_2(k) = (2,1)\mathbb{Z} + k(1,4)\mathbb{Z}.$$

The index of $\Gamma_2(k)$ is $7k$. A simple calculation shows that a point with period $\Gamma_2(k)$ is determined by three group elements, $a = x_{(0,0)}$, $b = x_{(1,1)}$, and $c = x_{(2,2)}$. The equations they must satisfy are described as follows. Let $A = \begin{bmatrix} 1 & 2 & 2 \\ 2 & 3 & 4 \\ 2 & 2 & 3 \end{bmatrix}$. Then the point with initial data $(a,b,c)$ specifies a point with period $\Gamma_2(k)$ if and only if

$$(a,b,c)A^k = (a,b,c). \tag{4}$$

The solution set to (4) has cardinality $G(R(k)) \times G(S(k)) \times G(T(k))$, where

$$\begin{bmatrix} R(k) & 0 & 0 \\ 0 & S(k) & 0 \\ 0 & 0 & T(k) \end{bmatrix}$$

is the integer Smith canonical form of the matrix $A^k - I$. Moreover, the group of points with period $\Gamma_2(k)$ is isomorphic to

$$\{g \in G \mid R(k)g = 0\} \times \{g \in G \mid S(k)g = 0\} \times \{g \in G \mid T(k)g = 0\}.$$

A sample of the calculations follows. The notation used on the right gives the numbers appearing in the integer Smith canonical form.

$$\begin{aligned}
\mathrm{Fix}_{\Gamma_2(1)}(\sigma^G) &= G(2) \times G(2) \times G(2) \\
\mathrm{Fix}_{\Gamma_2(2)}(\sigma^G) &= G(4) \times G(4) \times G(4) \\
\mathrm{Fix}_{\Gamma_2(3)}(\sigma^G) &= G(2) \times G(2) \times G(86) \\
\mathrm{Fix}_{\Gamma_2(4)}(\sigma^G) &= G(8) \times G(8) \times G(40) \\
\mathrm{Fix}_{\Gamma_2(5)}(\sigma^G) &= G(2) \times G(2) \times G(4, 762) \\
\mathrm{Fix}_{\Gamma_2(6)}(\sigma^G) &= G(4) \times G(4) \times G(8, 428) \\
\mathrm{Fix}_{\Gamma_2(7)}(\sigma^G) &= G(2) \times G(2) \times G(240, 494) \\
\mathrm{Fix}_{\Gamma_2(8)}(\sigma^G) &= G(16) \times G(16) \times G(26, 960) \\
\mathrm{Fix}_{\Gamma_2(9)}(\sigma^G) &= G(2) \times G(2) \times G(12, 354, 674) \\
\mathrm{Fix}_{\Gamma_2(10)}(\sigma^G) &= G(4) \times G(4) \times G(22, 105, 204).
\end{aligned}$$

A computer search produces the following: the determinant of $A^{117} - I$ is divisible by 3511 but not by $3511^2$;

$$\mathrm{Fix}_{\Gamma_2(117)}(\sigma^G) = G(54) \times G(54) \times G(3511 \times Q),$$

where the prime factorization of $Q$ is

$$Q = 2 \cdot 3^3 \cdot 19 \cdot 43 \cdot 79 \cdot 911 \cdot 1873 \cdot 7561 \cdot 555829 \cdot 659569 \cdot 869779 \cdot 66830177233$$

$$\cdot 330416497321 \cdot 31439667299041 \cdot 102533201268315620704903.$$

It follows that $G(3511)$ may be determined from the number of points with period $\Gamma_2(117)$; since 3511 divides exactly twice into $2^{3510} - 1$ the period $\Gamma_1(3510)$ determines $G(3511^2)$.

Now write $p$ for the prime 3511. We wish to show that the sequence $\{a_n = \det(A^n - I)\}$ is $p$–good. Write $\mathbb{C}_p$ for the algebraic closure of $\mathbb{Q}_p$, and $|\cdot|_p$ for the $p$–adic norm extended to $\mathbb{C}_p$. The matrix $A$ diagonalises over $\mathbb{C}_p$, the algebraic closure of $\mathbb{Q}_p$ into

$$D = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix}$$

where $\lambda_1 = 2687 + 2429p + 2936p^2 + O(p^3) \in \mathbb{Q}_p$ and $\lambda_2, \lambda_3 \in \mathbb{C}_p \backslash \mathbb{Q}_p$ are the roots of the equation

$$\lambda^2 + \lambda(2680 + 2429p + 2936p^2 + O(p^3)) + (98 + 2151p + 1907p^2 + O(p^3)) = 0.$$

It follows (as in Lemma 4) that $|\lambda_1^{117}-1|_p = p^{-1}$, $|\lambda_1^{117p}-1|_p = p^{-2}$ and so on. On the other hand, since for $j=2,3$ we have $|\lambda_j^{117}-1|_p = 1$, it follows that $|\lambda_j^{117p^r}-1|_p = 1$ for all $r$, so $|a_{117p^r}|_p = p^{-(r+1)}$. This shows that $\{a_n\}$ is 3511–good.

(4) The prime 1093.

For a history of this number and references, see [4]. Now let $\Gamma_3(k)$ be the finite index subgroup of $\mathbb{Z}^2$ defined by

$$\Gamma_3(k) = k(7,0)\mathbb{Z} + (0,2)\mathbb{Z}.$$

The index of $\Gamma_3(k)$ is $14k$. A calculation shows that a point with period $\Gamma_3(k)$ is determined by seven group elements, $(x_{(j,0)})_{j=0,\ldots,6}$. As above, the relations they must satisfy are given by the integer Smith canonical form of the matrix $B^k - I$; the matrix in this case is the circulant

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 2 \\ 2 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 1 \end{bmatrix}.$$

A computer search reveals that $\det(B^{39}-I)$ is divisible exactly once by 1093. As in case (3), we wish to deduce that the sequence $\{b_n = \det(B^n - I)\}$ is $p$–good for $p = 1093$. In this case the eigenvalues of $B$ all lie in $\mathbb{Q}_p$: they are given by $\{166+907p+O(p^2), \lambda = 514+844p+O(p^2), 16+930p+O(p^2), 100+834p+O(p^2), 4+0p+O(p^2), 784+890p+O(p^2), 609+1058p+O(p^2), 609+1058p+O(p^2)\}$. Then $|\lambda^{39}-1|_p = p^{-1}$; for $\mu$ any of the other six eigenvalues $|\mu^{39}-1|_p = 1$. It follows by the same argument that $\{b_n\}$ is 1093–good.

(5) The prime 2.

From the Smith form calculations in (3) above, we see that $G(2^n)$ is determined for $n = 1,2,3$ and 4. By Lemma 2, this suffices to determine the structure of the 2–primary component of $G$. Notice that we need the Smith form rather than the determinant in this case. □

## 3. Non–Abelian alphabet

The Conjecture in Section 1 makes sense without the assumption that the alphabet groups be abelian.

**Example.** Groups of order $p^3$, $p$ an odd prime. If $G$ has this order, then $G$ is one of five possible groups (see [13], Chapter IV,§3):

(1) $\langle x \mid x^{p^3} = 1\rangle$,
(2) $\langle x, y \mid x^{p^2} = y^p = 1, xy = yx\rangle$,
(3) $\langle x, y, z \mid x^p = y^p = z^p = 1, xy = yx, xz = zx, yz = zy\rangle$,
(4) $\langle x, y \mid x^{p^2} = y^p = 1, yxy^{-1} = x^{1+p}\rangle$,
(5) $\langle x, y \mid x^p = y^p = [x,y]^p = [x[x,y]] = [y,[x,y]] = 1\rangle$.

For non–abelian alphabets, the calculation of the number of points with period $\Gamma_1(k)$ is unaffected. It follows that for $p$ not a Wieferich prime, the periodic point data will distinguish between any two of the above groups except (3) and (5), both of which have exponent 3.

On the other hand, the periodic point data counts numbers of solutions to certain families of equations in several variables in the group $G$, and these numbers give more information than simply the number of elements of each order.

**Example.** If $\mathbf{x}$ is a point in $X_G$ with period $(2,0)\mathbb{Z} + (1,2)\mathbb{Z}$, and $x = x_{(0,0)}$, $y = x_{(1,0)}$ then $\mathbf{x}$ is determined by the pair $(x, y)$ and this pair satisfies the pair of equations

$$yx^2y = x, \quad xy^2x = y.$$

Consider monomials $w$ in finitely many non–commuting variables $x_1, x_2, \ldots, x_n$. To each finite set $\{w_1, \ldots, w_s\}$ of monomials, associate a number $G(w_1, \ldots, w_s)$ as follows: let $n$ be the largest number of variables appearing in any of the $w_i$, and put

$$G(w_1, \ldots, w_s) = |\{(g_1, \ldots, g_n) \in G^n \mid w_i(g_1, \ldots, g_n) = e \text{ for } i = 1, \ldots, s\}|.$$

Thus, the number of points with a given period determines $G(w_1, \ldots, w_s)$ for certain monomials $w_1, \ldots, w_s$.

**Lemma 6.** *Let $G$ be any finite group. Then the numbers $G(w_1, \ldots, w_s)$ for all words $w_1, \ldots, w_s$ and all $s$ together determine the group $G$ up to isomorphism.*

*Proof.* See Appendix. □

It follows that a non–abelian counter–example to the Conjecture, if it exists, must involve consideration of the specific equations determined by periodicities.

**Remarks.** (1) It is clear that higher powers of 2 can be dealt with simply by larger calculations, but finding a family of periods that will dispose of all powers of 2 at once has not been possible. This would involve finding the right power of 2 in the determinant, not just in the Smith form terms.
(2) The extension to all powers of the primes in cases (3) and (4) of Theorem 5 above may be shown equally well using arguments over the finite field $\mathbb{F}_p$.

## Appendix

*Proof of Lemma 2.* We can assume that $G$ is $p$–primary. If $p^{2n+2} \| |G|$ then the structure cannot be determined. To see this, let $G_1 = C_{p^{n+1}} \times C_{p^{n+1}}$ and $G_2 = C_{p^n} \times C_{p^{n+2}}$. Then $G_1(p^j) = G_2(p^j) = p^{2j}$ for $j = 1, \ldots, n$.

Now let $G$ have order $p^r$ for some $r \leq 2n + 1$. The structure of $G$ is determined up to isomorphism by a corresponding additive partition $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_k)$ of $r$ (the group corresponding to that partition being $G(\boldsymbol{\lambda}) = C_{p^{\lambda_1}} \times \cdots \times C_{p^{\lambda_k}}$). For each

$m$, define a function $\Phi_m$ on partitions by $\Phi_m(\boldsymbol{\lambda}) = \sum_{j=1}^{k} \min\{m, \lambda_j\}$. Then we have

$$G(\boldsymbol{\lambda})(p^m) = p^{\Phi_m(\boldsymbol{\lambda})}. \tag{5}$$

To prove the lemma, it is therefore enough to show that for a fixed unknown partition $\boldsymbol{\lambda}$, knowledge of the values $\Phi_1(\boldsymbol{\lambda}), \ldots, \Phi_n(\boldsymbol{\lambda})$ determines $\boldsymbol{\lambda}$ uniquely.

First notice that $\Phi_1(\boldsymbol{\lambda})$ is the number of nonzero terms in $\boldsymbol{\lambda}$: in the above notation, $\Phi_1(\boldsymbol{\lambda}) = k$. The next number $\Phi_2(\boldsymbol{\lambda})$ is twice the number of $\lambda_j$ in $\boldsymbol{\lambda}$ greater than or equal to 2 plus the number of $\lambda_j$ greater than or equal to 1, so $\Phi_2(\boldsymbol{\lambda}) - \Phi_1(\boldsymbol{\lambda}) = |\{j \mid \lambda_j \geq 2\}|$. In the same manner, $\Phi_\ell(\boldsymbol{\lambda}) - \Phi_{\ell-1}(\boldsymbol{\lambda}) = |\{j \mid \lambda_j \geq \ell\}|$. From these equations for $\ell \leq n$ we deduce that $|\{j \mid \lambda_j = 1\}| = 2\Phi_1(\boldsymbol{\lambda}) - \Phi_2(\boldsymbol{\lambda})$, $|\{j \mid \lambda_j = 2\}| = \Phi_1(\boldsymbol{\lambda}) - 2\Phi_2(\boldsymbol{\lambda}) + \Phi_3(\boldsymbol{\lambda})$, and so on up to $|\{j \mid \lambda_j = n-1\}| = \Phi_{n-2}(\boldsymbol{\lambda}) - 2\Phi_{n-1}(\boldsymbol{\lambda}) + \Phi_n(\boldsymbol{\lambda})$. Finally, the number $|\{j \mid \lambda_j = n\}|$ can be determined because $\boldsymbol{\lambda}$ is a partition of $r \leq 2n+1$: there can be at most 2 of the $\lambda_j$ that are greater than or equal to $n$. If there are no such $\lambda_j$, then the data above determine the partition. If there is one, it is determined by noting that the sum of all the $\lambda_j$ is $r \leq 2n+1$. If there are two such $\lambda_j$, then this will be detected because they will either both be $n$, with one other partition element being 1, or there will be one $\lambda_j$ equal to $n$ and no others found with size smaller than $n$, giving the unique solution $\boldsymbol{\lambda} = (n, n+1)$. In any case, the partition $\boldsymbol{\lambda}$ is determined. □

*Proof of Lemma 6.* Certainly the given data determines the order of $G$: it is $\max_{i \in \mathbb{N}}\{G(v_i)\}$, where $v_i = x_1^i$.

Let $F$ be the finitely presented group

$$F = \langle x_1, \ldots, x_n \mid w_1(x_1, \ldots, x_n) = e, \ldots, w_s(x_i, \ldots, x_n) = e \rangle$$

with generators $x_1, \ldots, x_n$ and relators $w_1, \ldots, w_s$. Each $n$–tuple $(g_1, \ldots, g_n) \in G^n$ with $w_i(g_1, \ldots, g_n) = e$ for $i = 1, \ldots, s$, determines a homomorphism $\Phi_{(g_1,\ldots,g_n)} : F \to G$ by setting $\Phi_{(g_1,\ldots,g_n)}(x_i) = g_i$ for all $i = 1, \ldots, s$. It is clear that this assignment determines a bijection between the set of all such $n$–tuples and the set of homomorphisms from $F$ to $G$. So the number of homomorphisms from $F$ to $G$ is exactly $G(w_1, \ldots, w_s)$. We therefore know, from the numbers $G(w_1, \ldots, w_s)$, the number of homomorphisms from $F$ to $G$ for each finitely presented group $F$. It follows that, for each finite group $K$, we know the number of homomorphisms from $K$ to $G$.

Fix $K$, and for each normal subgroup $N$ of $K$, let $a_K(N)$ be the number of homomorphisms from $K/N$ to $G$. By the above remark, all the numbers $a_K(N)$ are known. Now let $b_K(N)$ denote the number of injective homomorphisms from $K/N$ to $G$ for each normal subgroup $N$ of $K$. Then

$$a_K(N) = b_K(N) + \sum_{N < M \leq K} b_K(M),$$

where the sum is over all normal subgroups $M$ of $K$ that properly contain $N$. Thus, $b_K(N)$ can be determined by induction on the index $|K/N|$. Eventually, $b_K(\{e\})$, the number of injective homomorphisms from $K$ to $G$, is determined.

Now assume that $G$ and $H$ have the property that

$$G(w_1, \ldots, w_s) = H(w_1, \ldots, w_s)$$

for all $w_1, \ldots, w_s$. Then, since there are injective homomorphisms from $G$ to $G$, there must also be injective homomorphisms from $G$ to $H$. Such an injective homomorphism must also be surjective since $G$ and $H$ have the same order. □

## References


[1] R. Crandall, K. Dilcher and C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. **66** (1997), 433–449.

[2] F. Ledrappier, *Un champ markovien peut être d'entropie nulle et melangeant*, Comptes Rendus Acad. Sci. Paris **Ser. A, 287** (1978), 561–562.

[3] R.G.E. Pinch, *Recurrent sequences modulo prime powers*, Cryptography and Coding III, Oxford Univ. Press, Oxford, 1993.

[4] P. Ribenboim, *"1093"*, Math. Intelligencer **5** (1983), 28–33.

[5] ———, *The Book of Prime Number Records*, Springer–Verlag, New York, 1988.

[6] K. Schmidt, *Algebraic ideas in ergodic theory*, C.B.M.S. Reg. Conf. Ser. in Math. **76** (1990).

[7] ———, *Dynamical Systems of Algebraic Origin*, Birkhaüser, Basel, 1995.

[8] M.A. Shereshevsky, *On the classification of some two–dimensional Markov shifts with group structure*, Ergod. Th. and Dyn. Sys. **12** (1992), 823–833.

[9] T.B. Ward, *Almost block independence for the three dot $Z^2$ dynamical system*, Israel J. of Math. **76** (1991), 237–256.

[10] ———, *Periodic points for expansive actions of $Z^d$ on compact abelian groups*, Bull. London Math. Soc. **24** (1992), 317–324.

[11] ———, *An algebraic obstruction to isomorphism of Markov shifts with group alphabets*, Bull. London Math. Soc. **25** (1993), 240–246.

[12] A. Wieferich, *Zum letzten Fermatschen Theorem*, J. für die reine und angewandte Math. **136** (1909), 293–302.

[13] H.J. Zassenhaus, *The Theory of Groups*, Chelsea, New York, 1949.


School of Mathematics, University of East Anglia, Norwich NR4 7TJ, U.K.